Pearson BTEC Level 3 Nationals Diploma, Extended Diploma

Window for supervised period:
Monday 6 January 2020 – Friday 24 January 2020

Supervised hours: 4 hours | Paper Reference **20158K**

Information Technology

Unit 11: Cyber Security and Incident Management

Part B

You must have:
Forensic_Analysis.rtf

Instructions

- **Part A** and **Part B** contain material for the completion of the set tasks under supervised conditions.
- There are 43 marks for **Part A** and 37 marks for **Part B**, giving a total mark for the set task of 80.
- **Part A** and **Part B** are specific to each series and this material must be issued only to learners who have been entered to take the tasks in the specified series.
- This booklet should be kept securely until the start of the 4-hour, **Part B** supervised assessment period.
- **Part A** will need to have been completed and kept securely before starting **Part B**.
- Both parts will need to be completed during the 3-week period timetabled by Pearson.
- **Part A** and **Part B** tasks must be submitted together for each learner.
- **Part A** materials must not be accessed during the completion of **Part B**.
- This booklet should not be returned to Pearson.
- Answer **all** activities.

Information

- The total mark for this paper is 37.

Turn over ▶

Pearson

Instructions to Invigilators

This paper must be read in conjunction with the unit information in the specification and the *BTEC Nationals Instructions for Conducting External Assessments (ICEA)* document. See the Pearson website for details.

Refer carefully to the instructions in this task booklet and the *BTEC Nationals Instructions for Conducting External Assessments (ICEA)* document to ensure that the assessment is supervised correctly.

Part A and **Part B** set tasks should be completed during the period of 3 weeks timetabled by Pearson. **Part A** must be completed before starting **Part B**.

The 4-hour, **Part B** set task must be carried out under supervised conditions.

The set task can be undertaken in more than one supervised session.

An electronic template for activity 4 is available on the website for centres to download for learner use.

Learners must complete this task on a computer using the templates provided and appropriate software. All work must be saved as PDF documents for submission.

Invigilators may clarify the wording that appears in this task but cannot provide any guidance in completion of the task.

Invigilators should note that they are responsible for maintaining security and for reporting issues to Pearson.

Maintaining Security

- Learners must not bring anything into the supervised environment or take anything out.
- Centres are responsible for putting in place appropriate checks to ensure that only permitted material is introduced into the supervised environment.
- Internet access is not permitted.
- Learner's work must be regularly backed up. Learners should save their work to their folder using the naming instructions indicated in each activity.
- During any permitted break, and at the end of the session, materials must be kept securely and no items removed from the supervised environment.
- Learners can only access their work under supervision.
- User areas must only be accessible to the individual learners and to named members of staff.
- Any materials being used by learners must be collected in at the end of each session, stored securely and handed back at the beginning of the next session.
- Following completion of **Part B** of the set task, all materials must be retained securely for submission to Pearson.
- **Part A** materials must not be accessed during the completion of **Part B**.

Outcomes for Submission

Each learner must create a folder to submit their work. Each folder should be named according to the following naming convention:

[Centre #]_[Registration number #]_[surname]_[first letter of first name]_U11B

Example: Joshua Smith with registration number F180542 at centre 12345 would have a folder titled

12345_F180542_Smith_J_U11B

Each learner will need to submit 2 PDF documents, within their folder, using the file names listed.

Activity 4: activity4_incidentanalysis_[Registration number #]_[surname]_[first letter of first name]

Activity 5: activity5_securityreport_[Registration number #]_[surname]_[first letter of first name]

An authentication sheet must be completed by each learner and submitted with the final outcomes.

The work should be submitted no later than 28 January 2020.

Instructions for Learners

Read the set task information carefully.

Plan your time carefully to allow for the preparation and completion of all the activities.

Your centre will advise you of the timing for the supervised period. It is likely that you will be given more than one timetabled session to complete these tasks.

Internet access is not allowed.

You will complete this set task under supervision and your work will be kept securely at all times.

You must work independently throughout the supervised assessment period and must not share your work with other learners.

Your invigilator may clarify the wording that appears in this task but cannot provide any guidance in completion of the task.

Part A materials must not be accessed during the completion of **Part B**.

Outcomes for Submission

You must create a folder to submit your work. Each folder should be named according to the following naming convention:

[Centre #]_[Registration number #]_[surname]_[first letter of first name]_U11B

Example: Joshua Smith with registration number F180542 at centre 12345 would have a folder titled

12345_F180542_Smith_J_U11B

You will need to submit 2 PDF documents, within your folder, using the file names listed.

Activity 4: activity4_incidentanalysis_[Registration number #]_[surname]_[first letter of first name]

Activity 5: activity5_securityreport_[Registration number #]_[surname]_[first letter of first name]

You must complete an authentication sheet before you hand your work into your invigilator.

BLANK PAGE

Set Task Brief

Brilliant Billboards

Ben Jacobson owns Brilliant Billboards (BB). It is a small but rapidly expanding business that supplies digital information services for events. BB is based in a small industrial unit in Milton Keynes. Ben also works from his home office in the nearby town of Bletchley.

For each event BB provides a network of display, control, and communications equipment to meet the needs of the client.

The material displayed at the event can be controlled by four methods.

1. Through the local server, situated at the event location and connected to the event LAN.
2. Via remote access to the local server from BB, using an app written by BB.
3. Through local wireless access to personal devices, using Wi-Fi and/or Bluetooth, depending on the device being used.
4. By keyboard / keypad access to some of the display devices.

Client brief

You advised Ben on cyber security matters for his trailer-based advertising system. When you gave him your Management Report he asked you to review the investigation of a cyber security incident that had happened last Saturday.

The incident occurred at an antiques and collectables fair where BB was supplying digital information services. **Figure 1** shows BB's setup plan for the fair. North is at the top of the plan.

The fair was located in a public park and was open from 0900 to 1700 each day for one week.

The park is owned by the town council and is often used as an event site. The site was enclosed by temporary fencing made from steel mesh panels with a plywood facing. There is a public car park on one side of the site. The other sides are grass with trees and bushes.

BB provided the network infrastructure, including:

- two touch screen information points
- four digital projectors and screens
- three flat display screens
- WiFi service for event staff and the public.

The incident involved unauthorised access to two of the digital projectors.

Charita Katuwal was the BB staff member on duty at the fair, at the time of the incident. Her colleague, Hakeem Tawfiq, was on his lunch break and conducted an investigation when he returned.

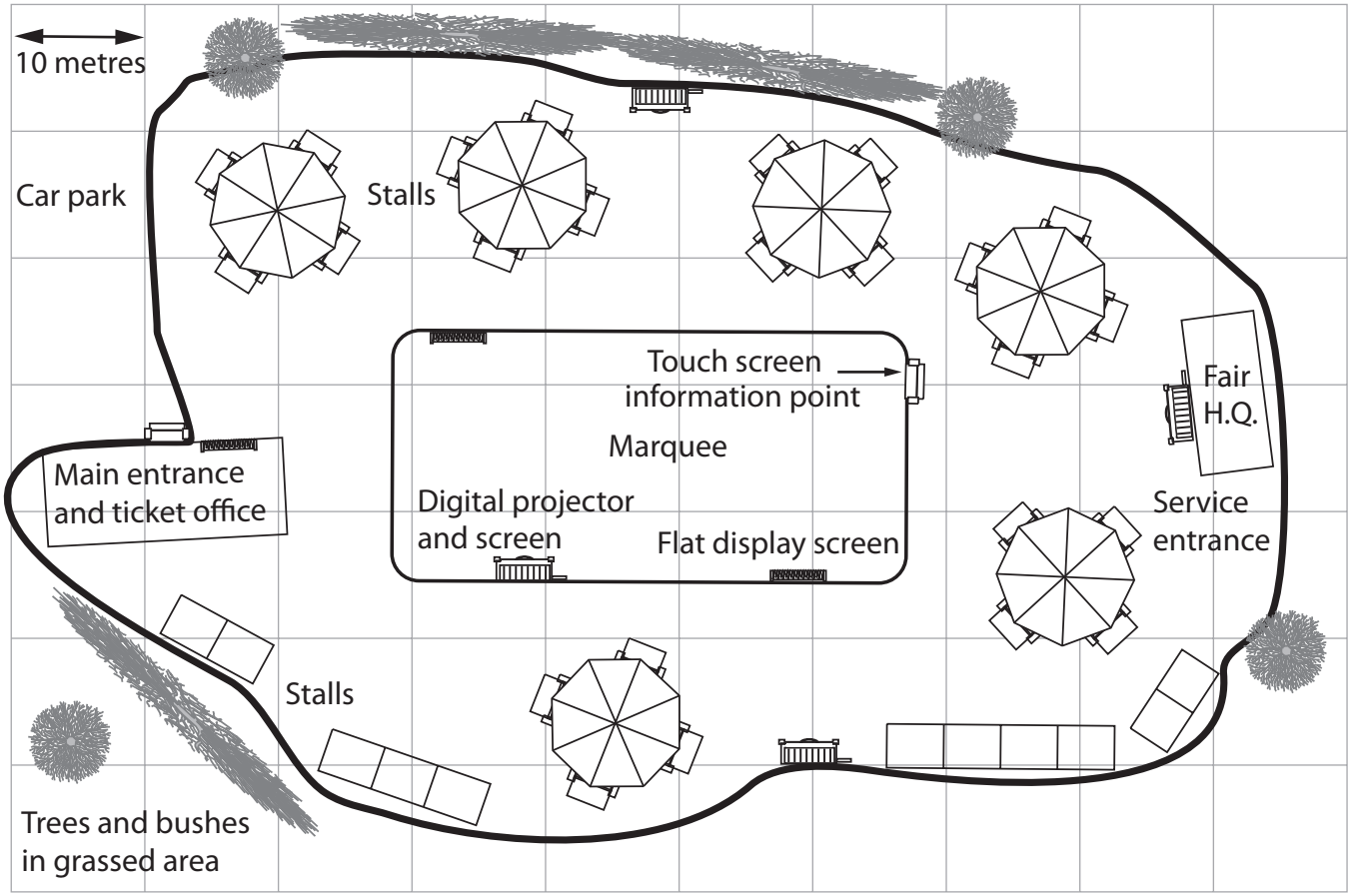


Figure 1

Evidence items from the security incident at the antiques and collectables fair

Evidence items include:

1) Charita's account
2) Hakeem's report
3) WiFi access logs
4) Network diagram
5) Cyber security document – incident management policy.

1) Charita's account

Today, Saturday, I was in the Fair HQ when I got a call from the ticket office saying that they were having a problem signing in to the event WiFi. I logged that at 13:25.

Hakeem was away getting lunch, so I left a note on his desk, logged into the WiFi to check that it was working, and then walked over to the ticket office.

It turned out that someone hadn't realised that the password was case sensitive and I was able to get them logged on without any problem.

On the way back to HQ, I noticed that the screen on the southern fence was showing some rude comments about the Fair. It was obviously not what was intended to be displayed. It had been showing normal event information when I passed it on my way to the ticket office.

I didn't have a Bluetooth projector controller with me, or the keys to the box containing the projector. I just used a piece of board to block the window where the projection shines through until I could get back to HQ and reset the display over the network.

As I was going into HQ, one of the stallholders ran up and said that the screen on the North wall, next to his stall, was displaying sequences of animated swear words. I went into HQ and immediately sent a reset command to the two projectors. I logged that at 13:35.

I'm more a network builder than an administrator, so I wasn't sure how to preserve logs and so on. But I thought it likely that the attack had been carried out over the WiFi and I managed to get the last ten minutes of activity displayed and took a screenshot **(see evidence item 3).**

Then I called Hakeem on his mobile and he got back at about 13:45 and took over the situation.

He asked me to go and remove the board from the southern projector, which I did, and then I made these notes.

2) Hakeem's report

Charita called me at 13:40, according to the call record on my mobile. She just said that there had been a problem with someone hacking into the system and that she thought that she'd fixed it but would I come and check as soon as I could. I reached HQ a few minutes later.

Charita gave an account of what had happened **(see evidence item 1)**. I thought that she'd handled things well and sent her to take the board away from the southern projector while I checked the system.

It seemed clear that the incident wasn't just someone getting in and playing with the system, the displays described by Charita must have been pre-prepared.

The attack took place in a period of less than ten minutes and there were no repeat attacks at the event.

I did not consider the incident to be serious enough to involve the police and there were no data protection implications.

I considered four ways in which the attack may have happened.

Intrusion via the Internet
Access logs for the event network didn't show any internet activity during the ten minutes before the incident. The ones for the public network had plenty of activity but there shouldn't be any way to access the projectors from that network.

Access via WiFi
Charita had taken screenshots of the WiFi logs for the ten minutes that covered the incident **(see evidence item 3)**. I had a look at the earlier records but couldn't see anything suspicious.

Physical access
I checked both projectors for signs that the changes may have been made by direct connection to their USB ports, but their protective boxes were still locked and there was no sign of tampering with the locks.

It's always possible that someone had got hold of a key but when I spoke to the stallholder he was sure that there hadn't been anyone near the projector when the display changed.

Bluetooth access
There are no logs for local Bluetooth links, so it may have been done that way. Although the culprit would have needed to be close to the projectors and there would have been a high risk of being seen. Unfortunately there was no CCTV covering the areas around the projectors.

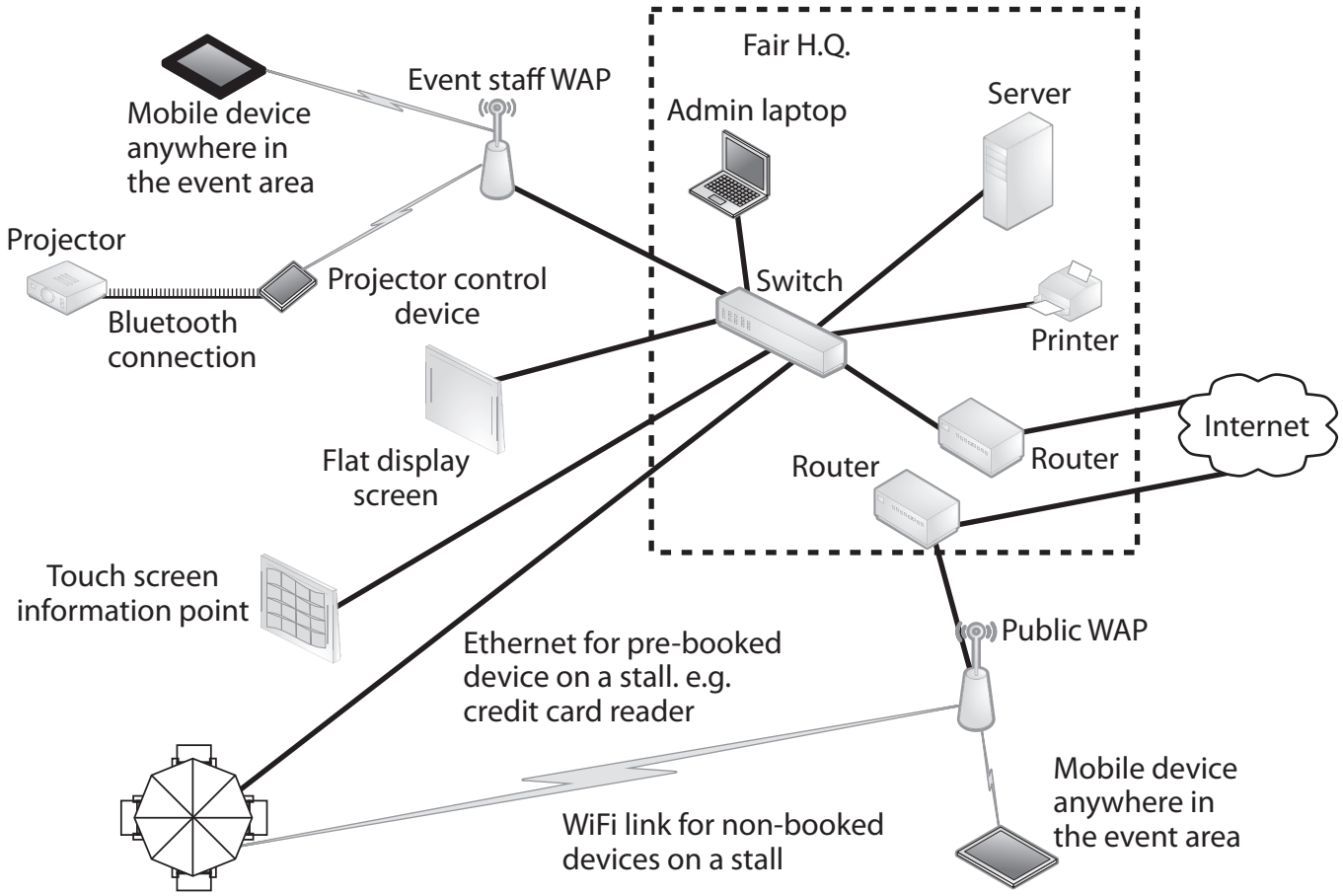
I concluded that this was a one-off, prank attack, possibly via Bluetooth. I changed the Bluetooth pairing codes for each of the projectors as a precaution.

3) WiFi access logs

Transcript of Public WiFi connection log Saturday 4th January.		
Time	**Event type**	**SSID**
13:26:05	connected	unicorn2
13:26:20	connected	ash_phone
13:26:54	connected	DFG64_wifi
13:28:15	disconnected	Shazaam
13:28:49	disconnected	Angela25
13:30:08	connected	kwall
13:31:22	disconnected	unicorn2
13:32:15	connection failed	unicorn2
13:32:40	connected	unicorn2
13:33:32	connected	megaman_16
13:33:36	connection failed	Jessie_the_best
13:33:51	connected	Jessie_the_best
13:35:02	disconnected	DFG64_wifi
13:36:19	disconnected	wizard_66

Transcript of BB Event WiFi connection log Saturday 4th January.			
Time	**Event type**	**SSID**	**Notes**
13:27:13	connected	BB_7	Charita login before leaving HQ
13:29:51	connected	Event_3	Event staff (ticket office)
13:31:45	login fail	unicorn2	No password
13:31:55	login fail	unicorn2	No password
13:34:05	disconnected	Event_3	Event staff (ticket office)
13:35:44	connected	Event_2	Event staff (security)
13:36:05	disconnected	BB_7	Charita logoff at HQ

4) Network diagram



5) Cyber security document – incident management policy

Incident management team

The team shall consist of:

- the network manager for incidents at BB's offices (team leader)
- the senior IT technician on site for incidents at an event (team leader)
- the technician who first responded to the incident
- Ben Jacobson, or a person designated by him (for incidents that involve outside authorities).

Incident reporting

Any member of staff who considers that an IT-related security incident has occurred must report it as soon as possible to the Computer Security Incident Response Team (CSIRT) leader.

Initially it may be reported verbally but this must be followed up by an email. It is the responsibility of the CSIRT to maintain detailed documentation on the incident from first report to final resolution.

Security incidents may include:

- theft of IT equipment
- theft of company data
- unauthorised access to company IT systems
- infection of company IT systems with malware.

Incident response procedures

(a) Theft of IT equipment

- Theft of IT equipment is a very serious issue. Any thefts must be reported at once to the CSIRT leader, initially a verbal report must be made followed up by email, providing as much information as possible (location and type of equipment, when it was last seen, etc.).
- The CSIRT leader must ascertain if the item has actually been stolen (or if it is just missing).
- If the item is confirmed as stolen, the CSIRT leader must inform the police and contact the finance department so they can inform insurers.
- The CSIRT must prepare a report on the theft to the directors and if needed justify the finances required to replace the stolen item.

(b) Theft of company data

- Theft or loss of company data equipment may occur in a number of different ways.
- Any loss of company data must be reported at once to the CSIRT leader, initially a verbal report must be made followed up by email.
- The CSIRT must investigate the loss and identify exactly what data has been lost or stolen and when the incident occurred.
- Having identified what has been lost or stolen and when, the CSIRT must retrieve backups and restore the data as soon as possible.
- The CSIRT should review the incident and implement procedures to prevent future losses.

(c) Infection of company IT systems with malware

- Any member of staff who suspects that any IT system has been infected with malware must report it at once to the CSIRT leader, initially a verbal report which must be followed up by email.
- The infected system should be shut down as soon as possible.
- The CSIRT will investigate the infection and take appropriate measures to resolve the infection and restore the system.

(d) Unauthorised access to company systems

- Any member of staff who suspects that there has been unauthorised access to any company IT system must report it at once to the CSIRT leader, providing as much detail as possible (which system, how access was obtained). Initially a verbal report must be made, followed up by email.
- The CSIRT will thoroughly investigate the incident and identify how the unauthorised access was obtained.
- The CSIRT will recommend action to prevent future occurrences (e.g. change passwords).

Part B Set Task

You must complete ALL activities within the set task.

Produce your documents using a computer.

Save your documents in your folder ready for submission using the formats and naming conventions indicated.

Read the set task brief carefully before you begin and note that reading time is included in the overall assessment time.

You have been advising Ben Jacobson on cyber security. Now he has asked you to review the investigation of a cyber security incident.

Activity 4: Forensic incident analysis

Analyse the forensic evidence, including how the evidence was obtained, for the cyber security incident at the antiques and collectables fair serviced by Brilliant Billboards (BB).

Consider possible causes of the incident and come to a conclusion about the most likely cause of the incident.

Refer to evidence items 1–4 inclusive.

Produce a forensic incident analysis using the template **Forensic_Analysis.rtf**

Save your completed forensic incident analysis as a PDF in your folder for submission as **activity4_incidentanalysis_[Registration number #]_[surname]_[first letter of first name]**

You are advised to spend 2 hours on this activity.

(Total for Activity 4 = 14 marks)

Activity 5: Security report

Review the incident. Suggest improvements and explain how they would prevent a similar incident in the future.

Areas for improvement are:

- adherence to forensic procedures
- the forensic procedure and current security protection measures
- the security documentation.

Read the set task brief and evidence items 1–5 inclusive when answering the question.

Save your completed security report as a PDF in your folder for submission as **activity5_securityreport_[Registration number #]_[surname]_[first letter of first name]**

You are advised to spend 2 hours on this activity.

(Total for Activity 5 = 20 marks)

TOTAL FOR TECHNICAL LANGUAGE IN PART B = 3 MARKS
TOTAL FOR PART B = 37 MARKS